UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/577,449	05/24/2000	Scott C. Harris	Biometrics	4716

23844 7590 09/02/2009

SCOTT C HARRIS
P O BOX 927649
SAN DIEGO, CA 92192

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2443	

NOTIFICATION DATE	DELIVERY MODE
09/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

scott@harrises.com
schuspto@gmail.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/577,449
Filing Date: May 24, 2000
Appellant(s): HARRIS, SCOTT C.

Scott C. Harris
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5-6-09 appealing from the Office action mailed 7-10-08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,035,398	**Bjorn**	3-2000
6,259,805	**Freedman et al.**	7-2001
6,002,787	**Takhar**	12-1999
6,714,665	**Hanna et al.**	3-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claim 26 and 28 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. There is no disclosure for the limitation of claim 26, "wherein the value identifies a portion of the scanned human body part among

the whole scanned human body part". There is no disclosure of the terms, "portion" or "whole" within the specification or the original claims.

There is no disclosure for the limitation of claim 28, "the received value identifies a feature of the fingerprint to be used by the encryption". The term, "feature", does not exist in the specification or the original claims. Appropriate correction required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims **26 - 31, 33 - 39, 41 - 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bjorn** (U.S. Patent No. **6,035,398**) in view of **Freedman et al.** (US Patent No. **6,259,805**) .

Regarding Claims 26, 37, Bjorn discloses a method of accessing files on a computer, comprising:

a) scanning a human body part to obtain information of the human body part that is indicative of at least one characteristic of the human body part; (Bjorn col 1, ll 39-42; col 3, ll 26-30; col 4, ll 4-7: generate biometric information utilized for user authentication, characteristic of human body part (fingerprint))

c) based on both the information indicative of the body part, and also on the value,

using the computer for obtaining a cryptographic key, by using only the portion of the scanned human body part identified by the received value to carry out at least a portion of the obtaining, and wherein the cryptographic key is used to enable a cryptographic operation which includes at least one of encryption or decryption of at least one file, on the computer; and

using the cryptographic key to carry out at least one of encryption and/or decryption of at least one file on the computer. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34: generation of cryptographic key utilizing biometric features; col 4, ll 30-46: generated key(s) utilized for encryption/decryption)

Bjorn does not explicitly disclose whereby receiving information indicative of a value known to the user, the value identifies a portion of the scanned human body part among the whole scanned human body part.

However, Freedman discloses:

b) receiving information indicative of a value known to the user, wherein the value has been entered by a user into the computer, and wherein the value identifies a portion of the scanned human body part among the whole scanned human body part; (Freedman col 11, ll 44-65: biometric information provided by individual is related to parameters selected; selects left ring finger, right thumb , and right index finger; biometric input means used to collect biometric information which are entered in a predetermined order; (biometric information input by user))

Specification discloses selection of multiple body parts in a precise order. (Specification Page 3, Lines 8-12) There no disclosure of a parameter that

identifies a portion of a scanned human body part.

It would have been obvious to one of ordinary skill in the art to modify Bjorn for a value that identifies a scanned human body part as taught by Freedman. One of ordinary skill in the art would have been motivated to employ the teachings of Freedman in order to reduce the time and expense of registration for authorized users, and to reduce the change of deriving a biometric template from poor biometric information. (Freedman col 4, ll 35-37: "*... For example, registration of authorized users requires little time and expense. The chance of deriving a biometric template from poor biometric information is greatly reduced. ...* ")

Regarding Claims 27, 38, Bjorn discloses a method as in claims 26, 37, wherein the scanning produces information which represents sufficient information about the human body part to render the information unique relative to other scanning of other body parts. (Bjorn col 3, ll 36-43: fingerprint information unique to fingerprint, comparison utilized for verification, (fingerprint uniqueness well known in the art))

Regarding Claim 28, Bjorn discloses a method as in claim 27, wherein the scanning comprises scanning a fingerprint to obtain information indicative of the fingerprint, and the received value identifies a feature of the fingerprint to be used by the encryption. (Bjorn col 1, ll 39-42; col 4, ll 4-7; col 3, ll 7-11: scan fingerprint utilizing sensor device)

There is no disclosure for this limitation: the received value identifies a feature of the fingerprint to be used by the encryption.

Regarding Claim 30, Bjorn discloses a method as in claim 27, wherein the human body part is scanned to produce digital information that is indicative of an analog image, and further comprising converting aspects of the analog image into digital information indicative of the cryptographic key. (Bjorn col 1, ll 52-55: fingerprint image (analog image); col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34: image converted into cryptographic key)

Regarding Claims 31, 41, Bjorn discloses a method as in claims 26, 37, wherein the forming a cryptographic key comprises first forming a first part of the cryptographic key using a first portion of the biometric information, subsequently and separately forming another part of the cryptographic key using another portion of the biometric information, and using both the one portion and the another portion of the biometric information together to form the cryptographic key. (Bjorn col 4, ll 13-24: cryptographic key generated utilizing some or all of biometric features information)

Regarding Claim 33, Bjorn discloses a method as in claim 31, wherein the forming comprises

a) obtaining the first part of the cryptographic key from the one portion of the biometric scan, (Bjorn col 4, ll 13-24: utilizing some or all of biometric features (curvature, ridge distance, etc.) for cryptographic key generation) and

b) obtaining the another part of the cryptographic key from the another portion

within the same biometric scan as the first portion, wherein the another portion is a different portion of the image than a first portion of image in which the one portion of the biometric scan is obtained. (Bjorn col 4, ll 13-24: utilize different portions (curvature, ridge distance, etc.) of fingerprint image for cryptographic key generation)

Regarding Claim 34, Bjorn discloses a method as in claim 31, wherein the forming comprises obtaining the first part of the cryptographic key from the one portion of the biometric scan, and getting the another part of the cryptographic key from the another portion within a different biometric scan from that scan that provides the first portion, wherein the another portion is based on a different image than a first image from which the one portion of the biometric scan is obtained. (Bjorn col 4, ll 13-24; col 4, ll 4-7: utilizing some or all of biometric features (curvature, ridge distance, etc.) information to generate cryptographic key; different biometric scans (fingerprint scans, different fingers))

Regarding Claims 35, 44, Bjorn discloses a method as in claims 34, 43, wherein the different biometric scan is a scan of a different body part than the part that provides the one portion. (Bjorn col 4, ll 4-7: different biometric body part, scan different finger (different body part, see specification page 7))

Regarding Claim 36, Bjorn discloses a method as in claim 26. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34; col 4, ll 30-46: generation of encryption/decryption key using biometric features) Bjorn does not explicitly disclose a retinal scan. However, Freedman discloses wherein the biometric scan includes a retinal scan. (Freedman col 9, ll 25-26; col 9, ll 51-55: retinal scan)

It would have been obvious to one of ordinary skill in the art to modify Bjorn where the biometric scan includes a retinal scan as taught by Freedman. One of ordinary skill in the art would have been motivated to employ the teachings of Freedman in order to reduce the time and expense of registration for authorized users, and to reduce the change of deriving a biometric template from poor biometric information. (Freedman col 4, ll 35-37

Regarding Claim 39, Bjorn discloses a system as in claim 38, wherein the first scanning part includes a fingerprint scanner. (Bjorn col 3, ll 7-11: fingerprint sensor (scanner))

Regarding Claim 42, Bjorn discloses a system as in claim 41, wherein the routine forms the first portion and the different portion of the image than a first portion of image in which the one portion of the biometric scan is obtained. (Bjorn col 4, ll 13-24: different portions of image (curvature, ridge distance, etc.) utilized for cryptographic key generation)

Regarding Claim 43, Bjorn discloses a system as in claim 41, wherein the routine forms the first portion and the another portion from different biometric scans, wherein the another portion is based on a different image than a first image from which the one portion of the biometric scan is obtained. (Bjorn col 4, ll 13-24: different portions of image (curvature, ridge distance, etc.) utilized for cryptographic key generation; col 4, ll 4-7: different biometric body part, scan a different finger (specification page 7))

Regarding Claims 45, 47, Bjorn discloses a method as in claims 27, 46, wherein the scanning comprises scanning a fingerprint to obtain information indicative of the fingerprint. (Bjorn col 1, ll 39-42; col 4, ll 4-7; col 3, ll 7-11: scan fingerprint utilizing sensor device)

Regarding Claim 46, Bjorn discloses a method, comprising:

a) scanning a human body part to obtain first information therefrom that uniquely represents the scanned body part; (Bjorn col 3, ll 7-11; col 4, ll 4-7: obtain fingerprint image, unique representation of body part)

c) forming third information from one portion of the first information, the one portion being along a different reference that the first information, and forming fourth information from another portion of the first information, the another portion being along a different reference than the first information; (Bjorn col 4, ll 13-20: portions of biometric information utilized to generate cryptographic key)

d) obtaining a cryptographic key based on all of the second information, the third

information, and the fourth information; (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34: generation of cryptographic key utilizing biometric features (some or all of features)) and

e) using the cryptographic key to carry out one of an encryption of information or a decryption of information on a computer. (Bjorn col 4, ll 30-46: keys utilized for encryption/decryption)

Bjorn does not explicitly disclose whereby receiving second information indicative of a value known to the user.

However, Freedman discloses:

b) receiving second information indicative of a value known to the user; (Freedman col 11, ll 44-65: biometric information provided by individual is related to parameters selected; selects left ring finger, right thumb , and right index finger; biometric input means used to collect biometric information which are entered in a predetermined order; (biometric information input by user))

Specification discloses selection of multiple body parts in a precise order. (Specification Page 3, Lines 8-12) There no disclosure of a parameter that identifies a portion of a scanned human body part.

It would have been obvious to one of ordinary skill in the art to modify Bjorn for receiving second information indicative of a value known to the user as taught by Freedman. One of ordinary skill in the art would have been motivated to employ the teachings of Freedman in order to reduce the time and expense of registration for authorized users, and to reduce the change of deriving a biometric template from

poor biometric information. (Freedman col 4, ll 35-37)

Regarding Claim 48, Bjorn discloses a method as in claim 46 and wherein the obtaining a cryptographic key comprises using the only a portion as a reference. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34; col 4, ll 30-46: generation of encryption/decryption key using biometric features) Bjorn does not explicitly disclose using the value to identify only a portion of the scanned human body part. However, Freedman discloses wherein further comprising using the value to identify only a portion of the scanned human body part. (Freedman col 11, ll 44-65: biometric information provided by individual is related to parameters selected; selects left ring finger, right thumb , and right index finger; biometric input means used to collect biometric information which are entered in a predetermined order; (biometric information input by user))

There no disclosure of a parameter that identifies a portion of a scanned human body part.

It would have been obvious to one of ordinary skill in the art to modify Bjorn for determining an average of values within the scanned body part and whether the values are greater than or less than the average as taught by Freedman. One of ordinary skill in the art would have been motivated to employ the teachings of Freedman in order to reduce the time and expense of registration for authorized users, and to reduce the change of deriving a biometric template from poor biometric information. (Freedman col 4, ll 35-37)

Regarding Claim 49, Bjorn discloses a method as in claim 26. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34; col 4, ll 30-46: generation of encryption/decryption key using biometric features) Bjorn does not explicitly disclose determining an average of values within the scanned body part and whether the values are greater than or less than the average. However, Freedman discloses wherein the using comprises determining an average of values within the scanned body part, and wherein the obtaining a cryptographic key operates based on whether the values are greater than or less than the average. (Freedman col 7, ll 5-13: scores for each characterized image, as template are averaged; score(s) are compared (greater than or less than) with a threshold (average, calculate parameter))

It would have been obvious to one of ordinary skill in the art to modify Bjorn for determining an average of values within the scanned body part and whether the values are greater than or less than the average as taught by Freedman. One of ordinary skill in the art would have been motivated to employ the teachings of Freedman in order to reduce the time and expense of registration for authorized users, and to reduce the change of deriving a biometric template from poor biometric information. (Freedman col 4, ll 35-37)

Regarding Claim 50, Bjorn discloses a system as in claim 37 and the running a routine obtains a cryptographic key. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34; col 4, ll 30-46: generation of encryption/decryption key using biometric features) Bjorn does

not explicitly disclose information indicative of characteristics of the human body part and whether the values are greater than or less than the average. However, Freedman discloses wherein the computer runs a routine that obtains information indicative of characteristics of the human body part and whether the values are greater than or less than the average. (Freedman col 7, ll 5-13: scores for each characterized image, as template are averaged; score(s) are compared with a threshold (average, calculate parameter))

It would have been obvious to one of ordinary skill in the art to modify Bjorn for information indicative of characteristics of the human body part and whether the values are greater than or less than the average as taught by Freedman. One of ordinary skill in the art would have been motivated to employ the teachings of Freedman in order to reduce the time and expense of registration for authorized users, and to reduce the change of deriving a biometric template from poor biometric information. (Freedman col 4, ll 35-37)

5. Claims **32, 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bjorn-Freedman** and further in view of **Takhar** (U.S. Patent No. **6,002,787**).

Regarding Claim 32, Bjorn discloses a method as in claim 27, wherein the forming uses the biometric information for a biometric authentication system. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34: biometric features utilized for cryptographic key generation) Bjorn does not explicitly disclose whereby forming uses the biometric

information to form information that is independent of any absolute dimensions in an image representing the biometric information. However, Takhar discloses wherein forming uses the biometric information to form information that is independent of any absolute dimensions in an image representing the biometric information. (Takhar col 26, ll 7-24; col 26, ll 38-41: ratios utilized for biometric parameter generation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bjorn-Hillhouse without determining absolute dimensions e.g. Ratios as taught in Takhar. One would have been motivated to utilize relationship e.g. Ratios between those parts in order to analyze fingerprint information, so that the obtained information be translated into the cryptographic key to allow access with accurate verification and to optimize cryptographic key generation. (Takhar col 1, ll 46-53)

Regarding Claim 40, Bjorn discloses a system as in claim 38, wherein the routine forms the cryptographic key by identifying a reference on the fingerprint, and using location of features on the fingerprint to the reference to obtain the biometric information. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34: biometric features utilized for cryptographic key generation) Bjorn does not explicitly disclose whereby a reference on the fingerprint, and using features relative to the reference to obtain the biometric information. However, Takhar discloses wherein a reference on the fingerprint, and using features on the fingerprint relative to the reference to obtain the

biometric information (Takhar col 26, ll 7-24; col 26, ll 38-41: ratios (relative information) utilized for biometric parameter generation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bjorn-Hillhouse without determining absolute dimensions e.g. Ratios as taught in Takhar. One would have been motivated to utilize relationship e.g. Ratios between those parts in order to analyze fingerprint information, so that the obtained information be translated into the cryptographic key to allow access with accurate verification and to optimize cryptographic key generation. (Takhar col 1, ll 46-53)

6. Claim **29** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Bjorn-Freedman** and further in view of **Hanna et al.** (U.S. Patent No. **6,714,665**).

Regarding Claim 29, Bjorn discloses a method as in claim 28, wherein the forming a cryptographic key comprises identifying a reference on the fingerprint, and using the received value to identify information within the fingerprint to obtain the biometric information. (Bjorn col 3, ll 32-34; col 4, ll 17-19; col 7, ll 32-34: generate cryptographic key from biometric information; col 4, ll 13-24: utilize locations on fingerprint in cryptographic key generation) Bjorn does not explicitly disclose a specified angle relative to a reference line. However, Hanna discloses wherein a specified angle relative to a reference line. (Hanna col 36, ll 5-9: reference line is with reference to an upright orientation; reference line used in angle analysis; col 49, ll 43-50: biometric

analysis; iris recognition)

It would have been obvious to one of ordinary skill in the art to modify Bjorn for a specified angle relative to a reference line as taught by Hanna. One of ordinary skill in the art would have been motivated to employ the teachings of Hanna in order to identify objects or individuals using a method that is both fast and accurate.. (Hanna col 1, ll 51-53: "*... This need makes clear that there exists a more general problem of identifying objects or individuals in a passive way that is both fast and accurate. ...* ")

(10) Response to Argument

The following ground(s) of rejection are applicable to the appealed claims:

A. Claims 26-31, 33-39, 41-50 stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman.

B. Claim 29 stands rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman and further in view of Hanna.

C. Claims 32 and 40 stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman and further in view of Takhar.

A. Claims 26-31, 33-39, 41-50 stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman.

The Office Action indicates that a 112 rejection for claims 26 and 28 has been written based on the lack of disclosure for the limitation *"wherein the value identifies a portion of the scanned human body part among the whole scanned human body*

part", and that the terms, *"portion"* or *"whole"*, are not disclosed in the specification or original claims.

The Office Action indicates that a 112 rejection for claim 28 has been written based on the lack of disclosure for the limitation *"a feature of the fingerprint to be used by the encryption"*, and that the term, *"feature"*, was not disclosed in the specification or original claims. There is no disclosure to use a feature of the fingerprint (a set of biometric information) in encryption.

A.1: Referenced prior art does not discloses: *"scanning a human body part tp obtaining characteristics of the human body part"*; ***"receiving information indicative of a value known to the user"***; *"based on both … said information … and said value … obtaining a cryptographic key"; and "using said cryptographic key". (Appeal Remarks Pages 12-20)*

Applicants' arguments specifically addressed *the value known to a user* limitation and its usage to create a set of biometric information.

Response to A.1:

The Examiner respectfully disagrees since Freedman discloses *"receiving information indicative of a value known to the user"*. The value also must be entered by the user into a computer system, and the value identifies a portion of a human body part. Even though Freedman allows the user to select (using an input value) which of their human body part will be scanned, the particular value indicating the selected biometrics is a parameter which is *known to the user* as the claim limitation requires.

The input parameter is used to select *"a portion of said scanned human body part"* such as a hand. Using this definition a specific finger is a portion of a hand or a portion of a human body part. .

Bjorn discloses the generation of a cryptographic key from a set of biometric information. The set of biometric information can be for a portion of a human body part such as a finger for a fingerprint. And, Freedman discloses the input of a parameter known to the user indicative of a body part (and indicating biometric information for a body part).

Both Bjorn and Freedman are in the same field of endeavor concerning usage of biometric information. Bjorn uses a set of biometric information to specifically generate a cryptographic key. Freedman uses the set of biometric information as an authentication mechanism. Both references utilize the same types of scanned biometric information. The set of biometric information generated in Freedman can be used to generate a key such as in Bjorn. Freedman indicates a motivation for the 103 combination of reducing the chances of deriving biometric information from poor quality biometric information. Achieved advantage is a valid motivation for the combination of prior art references.

A.2: Referenced prior art does not discloses for Claim 28 that the limitation *"specifies the received value identifies a feature of the fingerprint to be used". (Appeal Remarks Page 20)*

Freedman discloses the input of a value as indicated above. (Freedman col 11, ll

44-65: biometric information provided by individual related to parameters selected; selects left ring finger, right thumb, and right index finger; biometric input means used to collect biometric information (biometric information input by user)) Bjorn does disclose the usage of a feature in the processing of biometric information. (Bjorn col 3, ll 26-35: biometric features of fingerprint; col 4, ll 17-19; col 4, ll 26-36; col 7, ll 32-34: generation of cryptographic key utilizing biometric features; col 4, ll 30-46: generated key(s) utilized for encryption/decryption)

B. Claim 29 stands rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman and further in view of Hanna.

B.1: Applicant argues that the referenced prior art does not disclose: *"received value identifies a specified angle relative to a reference line for the fingerprint". (Appeal Remarks Page 24)*

Response to B.1:

Freedman discloses the input or receipt of a value as indicated above. Hanna discloses modifying a value to identify a specific angle relative to a reference line in the generation of biometric information. (Hanna col 36, ll 5-9: reference line is with reference to an upright orientation; reference line used in angle analysis; col 49, ll 43-50: biometric analysis; iris recognition) Hanna is used to disclose the usage of these types of parameters. (Hanna col 36, ll 5-9: reference line is with reference to an upright orientation; reference line used in angle analysis; col 49, ll 43-50: biometric analysis; iris recognition) And, Bjorn is used to disclose the generation of a cryptographic key from a

set of biometric information. (Bjorn col 3, ll 32-34; col 4, ll 17- 19; col 7, ll 32-34: generation of cryptographic key utilizing biometric features; col 4, ll 30-46: generated key(s) utilized for encryption/decryption)

C. Claims 32 and 40 rejected stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman and further in view of Takhar.

C.1: Applicant argues that the referenced prior art does not disclose *using ratios in processing a biometric scan. (Appeal Remarks Page 25)*

Response to C.1:

Takhar discloses the usage of relative dimensions or a ratio for a parameter instead of absolute dimensions in the processing of biometric information. Takhar is not used to disclose the generation of a cryptographic key. Takhar is only used to disclose the usage of relative dimensions for parameters. Bjorn is used to disclose the generation of a cryptographic key from a set of biometric information.

Conclusions

Bjorn discloses forming a key from a set of biometric information. Freedman discloses the identification of a portion of a body part as a set of biometric information. Freedman discloses that a selection of biometric information is made. The biometric information can be a fingerprint and/or a retinal scan. Bjorn and Freedman disclose the formation of a key using a part or a portion of a body part as the set of biometric

information. In addition, Freedman discloses a system for the input of a parameter associated with a particular body part. Bjorn and Freedman disclose functions equivalent to the claimed invention.

The claimed invention discloses the usage of parameters with relative dimensions as opposed to absolute dimensions such as in claims 32 and 40. The specification does not disclose the term "ratio" but does disclose the concept of relative instead of absolute dimensions and the original claims disclosed the term "ratios" in the usage of parameters. Takhar discloses the usage of ratio parameters which are relative measurements. The cited sections in Takhar disclose ridge to valley ratios or relative parameter operations in the analysis of a biometric fingerprint.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Kyung Hye Shin/ **8-20-2009**

Examiner, Art Unit 2443

Conferees:

/George C Neurauter, Jr./

Primary Examiner, Art Unit 2443

/Tonia LM Dollinger/
Supervisory Patent Examiner, Art Unit 2443